Digitalverbund Bayern

HITS IS – Hochschulübergreifender IT-Service Informationssicherheit

Notfallmanagement

Hochschulübergreifender IT-Service Informationssicherheit

Digitalverbund Bayern

Christian S. Fötinger

HITS IS – Hochschulübergreifender IT-Service Informationssicherheit

Kontakt und Information:

informationssicherheit@digitalverbund.de

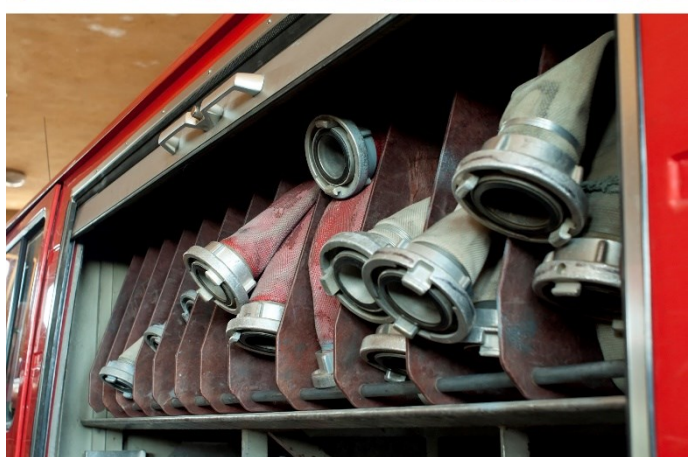
https://digitalverbund.bayern/hits/informationssicherheit/

Feuerlöscher?

Quelle: colourbox

Oder so?

- Feuerhemmende Ausstattung, Brandabschnitte
  - Teppich, Kabel, Mülleimer, Möbel, Räume, …
- Brandmelder (-detektoren)
- Brandschutzaushang an jeder Türe
- Fluchtwege gekennzeichnet
- Definiertes, geschultes Personal
- Übungen



Quelle: Colourbox

Brand vs. Cyberangriff

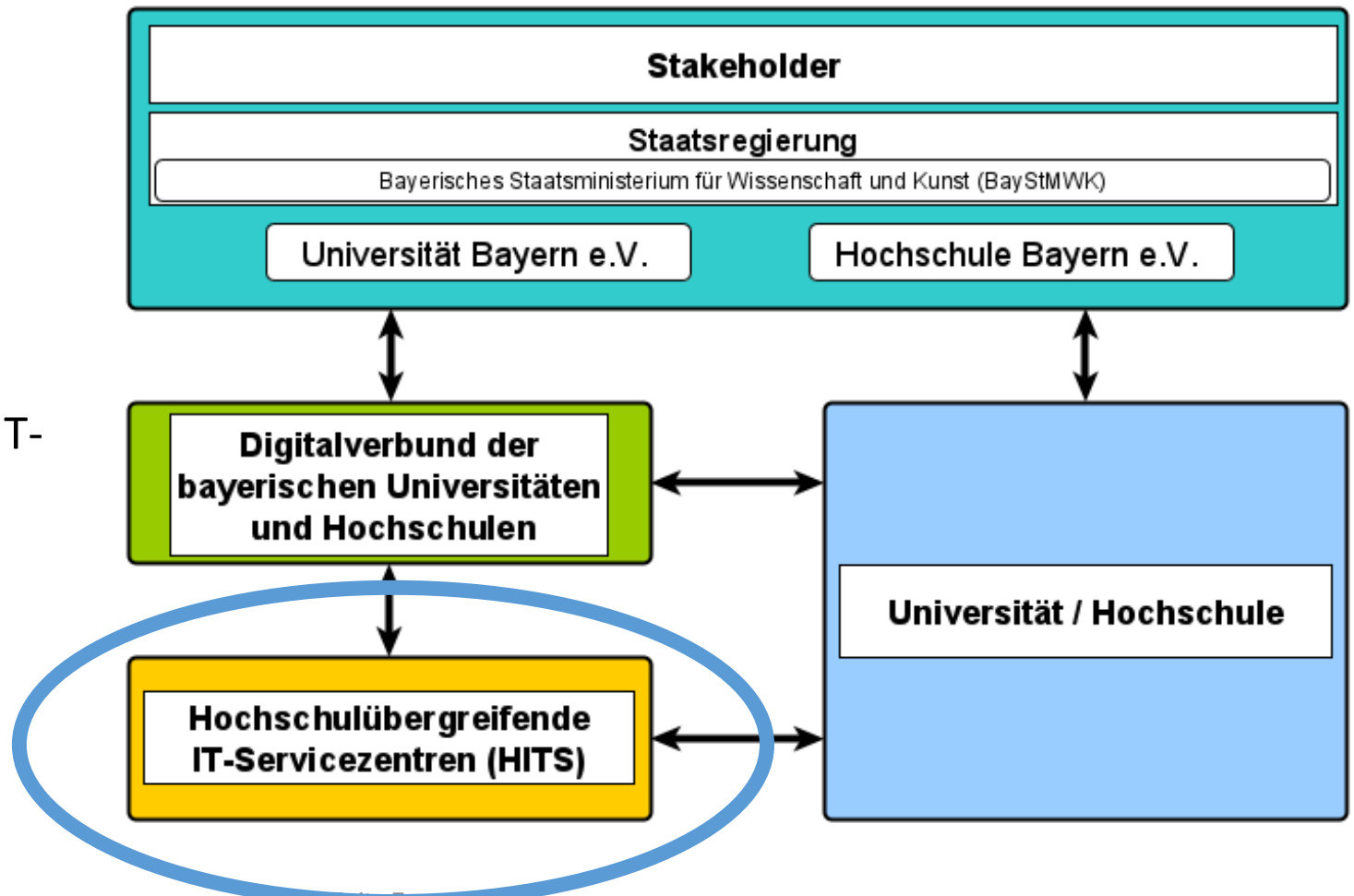
Brand	Cyberangriff
Feuerhemmende Ausstattung, Brandabschnitte	Virenschutz, Firewall, Rechtesystem
Brandmelder (-detektoren)	Protokolle, Meldung Service Desk, Analysen
Feuerlöscher	Software-Tools, Forensik
Brandschutzaushang (an jeder Bürotüre)	Verhaltensregeln (gesamtes Personal)
Fluchtwege gekennzeichnet	Notfallplan (u.a. welche Systeme weiterlaufen)
Definiertes, geschultes Personal	Notfallmanager, Einsatzteam, Krisenstab
Übungen	Übungen, Überprüfung der Rechte, Kontrolle

Alles bestens!

Digitalverbund Bayern

Digitalverbund

- Kooperative Vertretung
- Unterstützung der Digitalisierung
- strategische Entwicklung
- hochschulübergreifende IT-Services (HITS)



Digitalverbund Bayern

Arbeitsbereiche und Projekte

Arbeitsbereiche

- Notfallmanagement/Incident Response
- Schwachstellenscans
- Security-Analysen
- ISMS Consulting & Tool
- Hochschulinformations-sicherheitsprogramm (HISP)
- Audits
- Awareness
- Kommunikation
- Security Services Portfolio

Aktuelle Projekte

- DSM/BCM/ISMS Tool Einführung
- Notfallmanagementschulungen
  - Intensiv/Überblick
- eduCSIRT Aufbau

3 Standorte

- Augsburg (TH & Universität)
- LRZ Garching (bei München)
- HS München

Digitalverbund Bayern

Schwachstellenscans

Angebot

- regelmäßige Scans (Monitoring und Kontrolle) punktuelle Schwachstellenbezogene Scans
- Bereitstellung technischer Infrastruktur
- Beratung (Welche Systeme, welche Scans)
- Bewertung der Kritikalität und Handlungsanweisen
- Erstellung von Lagebildern

Externe Scans

Aus dem Internet erreichbare Systeme

Interne Scans

Innerhalb der Hochschulnetze

Ziel

- Minimierung der Angriffsflächen
- Identifizierung von veralteten, anfälligen Systemen
- Schutz vor zukünftigen Angriffen

BSI 200-4 Standard

- Initiierung des BCM-Prozesses
- Business Impact und Risikoanalyse
- Notfallpläne
- Notfallbewältigung
- Notfälle üben und kontinuierliche Verbesserung

Initiierung des BCMs – Überblick

Aufgaben der Institutsleitung

- Übernahme der Gesamtverantwortung für BCM → Leitlinie
- Bereitstellung der BCM Ressourcen
- Benennung des BC-Beauftragten u. Einbindung der Mitarbeiter in den Prozess

Dokumente

- Leitlinie
- Notfallvorsorgekonzept (Rollen, Prozess, Dokumente)

Business Impact Analyse

- Vorarbeit: Geschäftsprozesse erfassen
- Schadensbewertung bei Ausfall des Prozesses

→ Zeitkritische Geschäftsprozesse und Ressourcen bestimmen

→ Unzureichend abgesicherte Ressourcen feststellen

Dokumente

Ergebnisse der Business Impact Analyse

BC-Strategien und Notfallpläne

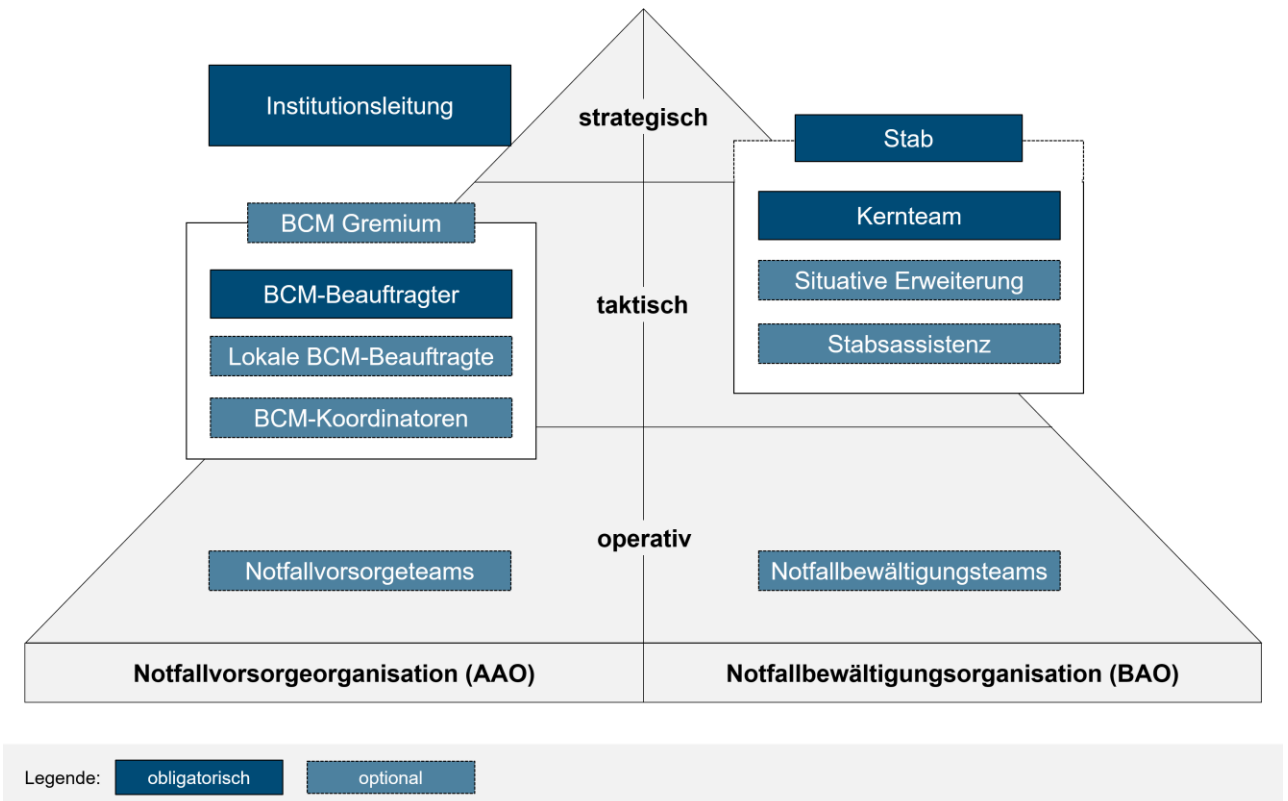
- Identifizierung von BC-Strategien (Umsetzungsplan)
- Maßnahmen werden in Notfallplänen ausgearbeitet

Notfallpläne

- Notfallhandbuch (übergreifend)
- Geschäftsfortführungspläne (je Organisationseinheit)
- Wiederanlauf- und Wiederherstellungspläne (je Ressource)

→ Offline Verfügbarkeit aller Dokumente!

Notfallbewältigungsteam



Aufrechterhaltung und Verbesserung

Regelmäßige Überprüfung des BCMs

- Notfallübungen (Jahresübungsplan)
- Fazit aus eingetretenen Notfällen und Krisen
- Kennzahlen- und Maßnahmenüberprüfung

Dokumente

- (Interne und externe) Revisionen, Berichte
- Aktualisierung der BCM-Dokumente

Business Continuity Management (BCM)

Workshop (Pilot)	Inhalte
BCM und Krisenkommunikation	Überblick über BCM Vorgehensweise mit Fokus auf BSI 200-4, inkl. Musterdokumente und Übungen zur Krisenkommunikation (Dauer ca. 6h)
BCM – Erste Schritte im BCM-Tool	Überblick über BCM Vorgehensweise im BCM-Tool (Dauer ca. 4h)
BCM in Kürze	Präsentation für Leitungsebene, Kurzüberblick (Dauer ca. 1h)

Digitalverbund Bayern

Laufendes Projekt - eduCSIRT

Projekt zum Aufbau eines Cyber Security Incident Response Teams (CSIRT) für die bayerischen Hochschulen

- Notfallinfrastruktur am LRZ Garching
  - Begrenzte Anzahl an Mailadressen
  - Filesystem
  - Chatprogramm
  - Notfallwebseite (zum Bloggen)
- Kontakt bei Cyberangriffen
  - Analyse des Vorfalls
  - Kontakt zu externen Dienstleistern (APT, Forensik)
- Notfallbudget

Forcierung folgender Dienste

- Begleitung einzelner Hochschulen
  - Informationssicherheit
  - Sensibilisierung
  - Notfallmanagement
- eduCSIRT (Notfalleinsatztruppe)
- Prüfungen (technisch und organisatorisch)

Erste Schritte

- BC-Beauftragten benennen (evtl. Schulung planen)
- Leitlinie ausarbeiten und freigeben
- Zusammensetzung des Stabs bestimmen
- Kritische Prozesse bestimmen
- Strategien entwickeln
- …
- Üben, üben, üben

Viel Erfolg